The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
03/14/2017

SUBJECT:
Multiple Vulnerabilities in Microsoft Uniscribe Could Allow for Remote Code Execution (MS17-011)

OVERVIEW:
Multiple vulnerabilities exist in Windows Uniscribe, the most severe of which could result in remote code execution. Uniscribe is a set of APIs that allow a high degree of control for fine typography and for processing complex scripts as well as supporting the display and editing of international text. Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are no reports of these vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:
- Microsoft Windows: Vista, 7, 8.1, RT 8.1, 10
- Microsoft Windows Server: 2008, 2008 R2, 2012, 2012 R2, 2016
- Microsoft Windows Server Core: 2008, 2008 R2, 2012, 2012 R2, 2016

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities exist in Windows Uniscribe, the most severe of which could result in remote code execution. The vulnerabilities are as follows:

- Multiple remote code execution vulnerabilities exist in Windows due to the way Windows Uniscribe handles objects in memory. (CVE-2017-0072, CVE-2017-0083, CVE-2017-0084, CVE-2017-0086, CVE-2017-0087, CVE-2017-0088, CVE-2017-0089, CVE-2017-0090)
- Multiple information disclosure vulnerabilities exist when Windows Uniscribe improperly discloses the contents of its memory. (CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, CVE-2017-0128)

Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments, especially those from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Microsoft:
https://technet.microsoft.com/library/security/MS17-011

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0072
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0083
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0084
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0085
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0086
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0087
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0088
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0089
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0090
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0091
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0092
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0111
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0112
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0113
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0114

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0115
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0116
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0117
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0118
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0119
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0120
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0121
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0122
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0123
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0124
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0125
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0126
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0127
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0128